



Broadcom

250-561

Endpoint Security Complete - R1 Technical Specialist

Questions & Answers PDF

For More Information:

<https://www.certswarrior.com/>

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 6.0

Question: 1

Which option should an administrator utilize to temporarily or permanently block a file?

- A. Delete
- B. Hide
- C. Encrypt
- D. Blacklist

Answer: D

Question: 2

Which report template includes a summary of risk distribution by devices, users, and groups?

- A. Device Integrity
- B. Threat Distribution
- C. Comprehensive
- D. Weekly

Answer: B

Question: 3

What does SES's advanced search feature provide when an administrator searches for a specific term?

- A. A search modifier dialog
- B. A search wizard dialog
- C. A suggested terms dialog
- D. A search summary dialog

Answer: A

Question: 4

In which phase of MITRE framework would attackers exploit faults in software to directly tamper with system memory?

- A. Exfiltration
- B. Discovery
- C. Execution
- D. Defense Evasion

Answer: D

Question: 5

An administrator suspects that several computers have become part of a botnet. What should the administrator do to detect botnet activity on the network?

- A. Enable the Command and Control Server Firewall
- B. Add botnet related signatures to the IPS policy's Audit Signatures list
- C. Enable the IPS policy's Show notification on the device setting
- D. Set the Antimalware policy's Monitoring Level to 4

Answer: A

Question: 6

Which Anti-malware technology should an administrator utilize to expose the malicious nature of a file created with a custom packet?

- A. Sandbox
- B. SONAR
- C. Reputation
- D. Emulator

Answer: A

Question: 7

An endpoint is offline, and the administrator issues a scan command. What happens to the endpoint when it restarts, if it lacks connectivity?

- A. The system is scanning when started.
- B. The system downloads the content without scanning.
- C. The system starts without scanning.
- D. The system scans after the content update is downloaded.

Answer: B

Question: 8

Which type of security threat is used by attackers to exploit vulnerable applications?

- A. Lateral Movement
- B. Privilege Escalation
- C. Command and Control
- D. Credential Access

Answer: B

Question: 9

What is the primary issue pertaining to managing roaming users while utilizing an on-premise solution?

- A. The endpoint is missing timely policy update
- B. The endpoint is absent of the management console
- C. The endpoint fails to receive content update
- D. The endpoint is more exposed to threats

Answer: C

Question: 10

What should an administrator know regarding the differences between a Domain and a Tenant in ICDm?

- A. A tenant can contain multiple domains
- B. A domain can contain multiple tenants
- C. Each customer can have one domain and many tenant
- D. Each customer can have one tenant and many domains

Answer: A



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ